REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)

2. REPORT DATE:

3. REPORT TYPE AND DATES COVERED
Final Report 1-Apr-2002 - 30-Sep-2005

4. TITLE AND SUBTITLE
Quantum Complexity, Algorithms, and Primitives

5. FUNDING NUMBERS
DAAD190210048

6. AUTHORS
Stephen A. Fenner

8. PERFORMING ORGANIZATION REPORT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of South Carolina
Office of Sponsored Programs & Research
James F. Byrnes International Center
Columbia, SC 29208 -

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

43511-PH-QC.1

11. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

The abstract is below since many authors do not follow the 200 word limit

14. SUBJECT TERMS
quantum computing, small-depth quantum circuits, quantum complexity classes, distribution-valued functioons, counting complexity, quantum algorithms on groups,

15. NUMBER OF PAGES
Unknown due to possible attachments

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
UNCLASSIFIED

18. SECURITY CLASSIFICATION ON THIS PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
UL

Report Title

Final Progress Report on "Quantum Complexity, Algorithms, and Primitives"

ABSTRACT

The project undertook theoretical research in quantum algorithms, complexity of quantum computation, quantum primitives, and quantum communication protocols. In the area of complexity, it compared quantum computation models with classical ones, finding counting complexity classes between BQP and AWPP that are likely different from both. It investigated small-depth quantum circuits (both with and without unbounded fan-in gates such as quantum AND) and found lower and upper bounds on their power and complexity. In the area of new quantum primitives, the project found Hamiltonians for the quantum fan-out gate, based on spin-exchange interactions. In the area of quantum algorithms, the project showed that there are efficient quantum algorithms for various group theoretic problems, for example, group intersection and double coset membership for certain classes of solvable groups. It also found a network of efficient quantum reducibilities between these and other group-theoretic problems. These are the project's successes.

The project was unsuccessful in some endeavors. It has so far failed to find natural problems in these intermediate classes between BQP and AWPP, or to isolate the more robust classes among these. It did not find further evidence that BQP does not contain NP. There was no significant progress on quantum communication protocols.

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Related to the project:

M. Fang, S. Fenner, F. Green, S. Homer, Y. Zhang. Quantum Lower Bounds for Fanout. Quantum Information and Computation. Volume 6 (2006), pages 46-57.

S. Fenner. PP-lowness and a simple definition of AWPP. Theory of Computing Systems. Volume 36 (2003) pages 199-212.

S. Fenner, L. Fortnow, S. Kurtz, L. Li. An oracle builder's toolkit. Information and Computation. Volume 182 (2003), pages 95-136.

Number of Papers published in peer-reviewed journals: 3.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

S. Fenner, Y. Zhang. Quantum Algorithms for a Set of Group Theoretic Problems. Proceedings of the Ninth IC-EATCS Italian Conference on Theoretical Computer Science, Siena, Italy, October 2005. Springer LNCS 3701, pages 215-227.

S. Fenner, F. Green, S. Homer, Y. Zhang. Bounds on the Power of Constant-Depth Quantum Circuits. Proceedings of the 15th International Symposium on Fundamentals of Computation Theory, Luebeck, Germany, August 2005. Springer LNCS 3623, pages 44-55.

S. A. Fenner, Y. Zhang. Implementing fanout, parity, and Mod gates via spin exchange interactions. E-print archive quant-ph/0407125, 2004.

S. Fenner. A Physics-Free Introduction to the Quantum Computation Model. In Current Trends in Theoretical Computer Science: The Challenge of the New Century, G. Paun, G. Rozenberg, A. Salomaa, eds. Volume 1 (Algorithms and Complexity). World Scientific, 2004, pages 125-145. An earlier version appeared in the Bulletin of the European Association for Theoretical Computer Science, 2003.

S. A. Fenner, Y. Zhang. A note on the classical lower bound for a quantum walk algorithm. E-print archive quant-ph/0312230, 2003.

S. A. Fenner. Implementing the fanout gate by a Hamiltonian. E-print archive quant-ph/0309163, 2003.

Number of Papers published in non peer-reviewed journals: 6.00

(c) Papers presented at meetings, but not published in conference proceedings (N/A for none)

S. Fenner, Y. Zhang. Implementing the Fanout Gate with Spin-Exchange Interactions. Invited talk at Theoretical Division colloquium, Los Alamos National Laboratory, Los Alamos, NM, September, 2004. Also invited talk at joint Physics and Computer Science colloquium, University of Calgary, Calgary, Alberta, CA, August, 2004.

Number of Papers not Published: 1.00

(d) Manuscripts

S. Fenner, Y. Zhang. Distribution-valued functions and quantum computation. 2003.

Number of Manuscripts: 1.00

Number of Inventions:

Graduate Students

Yong Zhang (60%)

Number of Graduate Students supported: 1.00

Total number of FTE graduate students: 1.00

Names of Post Doctorates

Number of Post Docs supported: 0.00

Total number of FTE Post Doctorates: 0.00

List of faculty supported by the grant that are National Academy Members

Names of Faculty Supported

Stephen A. Fenner

Number of Faculty: 1.00

Names of Under Graduate students supported

Number of under graduate students: 0.00

Names of Personnel receiving masters degrees

Yong Zhang

Number of Masters Awarded: 1.00

Names of personnel receiving PHDs

Yong Zhang

Number of PHDs awarded: 1.00

Names of other research staff

Sub Contractors (DD882)

Inventions (DD882)

Final Technical Report for ARO Contract DAAD 190210048

Stephen A. Fenner

December 31, 2005

Abstract

The project undertook theoretical research in quantum algorithms, complexity of quantum computation, quantum primitives, and quantum communication protocols. In the area of complexity, it compared quantum computation models with classical ones, finding counting complexity classes between **BQP** and **AWPP** that are likely different from both. It investigated small-depth quantum circuits (both with and without unbounded fan-in gates such as quantum AND) and found lower and upper bounds on their power and complexity. In the area of new quantum primitives, the project found Hamiltonians for the quantum fan-out gate, based on spin-exchange interactions. In the area of quantum algorithms, the project showed that there are efficient quantum algorithms for various group theoretic problems, for example, group intersection and double coset membership for certain classes of solvable groups. It also found a network of efficient quantum reducibilities between these and other group-theoretic problems. These are the project's successes.

The project was unsuccessful in some endeavors. It has so far failed to find natural problems in these intermediate classes between **BQP** and **AWPP**, or to isolate the more robust classes among these. It did not find further evidence that **BQP** does not contain **NP**. There was no significant progress on quantum communication protocols.

Contents

List of Figures

1 Statement of Problems Studied

The project investigated the following questions:

1. **Are there natural, robust complexity classes between BQP and AWPP that are unlikely to be equal to either? AWPP** is a counting class defined by Li [Li93, FFKL03] and shown to include **BQP** by Fortnow & Rogers [FR99]. It the smallest well-studied non-quantum class known to contain **BQP**.

2. **Is there more convincing evidence that NP $\not\subseteq$ BQP?** This noninclusion would imply that **NP**-complete problems are not tractable even with a quantum computer.

3. **What is the power of families of quantum circuits of small depth, especially sub-logarithmic or constant depth?** This is an open-ended question whose answer depends on several independent variables, for example, which types of gates are allowed, how much error probability is allowed, and how may ancilla qubits are allowed.

4. **How easily can small-depth quantum circuits be simulated, either classically, or by more restricted quantum circuits?** This question is closely related to the previous one.

5. **Are there quantum operations that can act as new primitives that are both algorithmically powerful and potentially physically feasible?** New quantum computational primitives may help to span the gap between theory and implementation of quantum computation.

6. **Can new quantum algorithms be found for problems believed to be classically intractable?** Good candidates for such problems include special cases of the well-studied Hidden Subgroup problem for nonabelian groups.

7. **What new communication protocols can be based on quantum information principles?**

The project was largely successful with items 3, 4, 5, and 6. It was somewhat successful with item 1, and largely unsuccessful with items 2 and 7. The project also had a result unrelated to the questions above (see Section 2.8).

2 Summary of Results

After some preliminary definitions, the project's results related to the above questions will be described in the same order as they are listed.

We let $\mathbb{N} = \{0, 1, 2, \ldots\}$ and fix $\Sigma = \{0, 1\}$ to be the standard binary alphabet. For $n \in \mathbb{N}$, we define Σ^n to be the set of all binary strings (strings over Σ) of length n. We let $\Sigma^* = \bigcup_{n \in \mathbb{N}} \Sigma^n$. We identify Σ^* with $\mathbb{N}$ via the usual binary representation. For $x, y \in \Sigma^*$ we let $|x|$ denote the length of x, and we write $x \sqsubseteq y$ to mean that x is a prefix of y. We use standard concepts and notation from computational complexity theory (see Papadimitriou [Pap94], for example).

2.1 Classes Between BQP and AWPP

We have defined a number of counting complexity classes between **BQP** and **AWPP** [Fen03a]. These classes are defined using distribution-valued functions similar to those used by Aharonov, Kitaev, & Nisan [AKN98] in defining the quantum function class **FQP**.

Definition 2.1. *A function f is a* distribution-valued function *(or* DVF*) if there is a polynomial p such that, for all $n \in \mathbb{N}$ and $x \in \Sigma^n$, $p(n) \geq 1$ and $f(x)$ is a probability distribution on $\Sigma^{p(n)}$. For $y \in \Sigma^{p(n)}$, we write $f(y \mid x)$ for the probability assigned to y by $f(x)$. For every $0 \leq m < p(n)$, $f(x)$ induces a natural probability distribution on Σ^m which assigns to each string $z \in \Sigma^m$ the probability*

$$f(z \mid x) = \sum_{y \in \Sigma^{p(n)} : z \sqsubseteq y} f(y \mid x).$$

For example, the distributions of output probabilities of a family of polynomial-size quantum circuits is a DVF of the inputs to the circuits. Such DVFs form the class **FQP**. We can define language classes based on **FQP** as follows:

Definition 2.2. *For any DVF f, we define the* language of f, *written L_f, to be such that, for all $x \in \Sigma^*$,*

$$x \in L_f \iff f(0 \mid x) > 1/2.$$

We say that f has bounded error *if for all $x \in \Sigma^*$ and $r \in \mathbb{N}$,*

$$f(0 \mid \langle x, 0^r \rangle) \leq 2^{-r} \ \text{ or } \ f(0 \mid \langle x, 0^r \rangle) \geq 1 - 2^{-r}.$$

We say that f is exact *if $f(0 \mid x) \in \{0, 1\}$ for all $x \in \Sigma^*$.*

Definition 2.3. *Let $\mathcal{F}$ be a class of distribution-valued functions. We define the* bounded error class of $\mathcal{F}$ *as*

$$\mathrm{B} \cdot \mathcal{F} = \{L_f : f \in \mathcal{F} \text{ has bounded error}\}.$$

We define the zero error class of $\mathcal{F}$ *as*

$$\mathrm{E} \cdot \mathcal{F} = \{L_f : f \in \mathcal{F} \text{ is exact}\}.$$

We get $\mathbf{BQP} = \mathrm{B} \cdot \mathbf{FQP}$ and $\mathbf{EQP} = \mathrm{E} \cdot \mathbf{FQP}$. We get bigger subclasses of **AWPP** by considering broader classes of DVFs than **FQP**. In particular, we define DVFs based on exponential size matrices whose entries are Gap**P** functions of the input (for information about Gap**P**, see [FFK94] for example).

Definition 2.4. *A DVF f is in the class* **FM** *if there is a polynomial $p \geq 1$, a function $g \in \mathrm{Gap}\mathbf{P}$, and a ptime computable function $h : \Sigma^* \to \mathbb{N}$ such that for all $n \in \mathbb{N}$, all $x \in \Sigma^n$, and all $y \in \Sigma^{p(n)}$ we have*

$$f(y \mid x) = \left(\frac{g(y,x)}{h(0^{|x|})} \right)^2 .$$

It is easy to show that $\mathrm{B} \cdot \mathbf{FM} = \mathbf{AWPP}$. This definition generalizes **FQP** by allowing the probability amplitude of an output state $|y\rangle$ given an input state $|x\rangle$ to be of the form $g(y,x)/h(0^{|x|})$. Let M be the $2^{p(n)} \times 2^{p(n)}$ matrix with (y,x) entry being $g(y,x)/h(0^{|x|})$. By restricting the form of M, we can obtain classes between **BQP** and **AWPP**. For example, let **FUM** be the class of DVFs in **FM** for which the matrix M is unitary (or orthogonal, since it is a real matrix), and let $\mathbf{BUM} = \mathrm{B} \cdot \mathbf{FUM}$. Then we have $\mathbf{BQP} \subseteq \mathbf{BUM} \subseteq \mathbf{AWPP}$, the first inclusion following from the fact that any quantum computation can be rendered by a circuit with real probability amplitudes, and it is known that these amplitudes can be of the form $g(y,x)/h(0^{|x|})$ [FR99]. Another possibility is to restrict the matrix M to be antisymmetric, letting the probability amplitudes be entries of the matrix $N = \exp(M)$. If we define **FAM** to be the corresponding class of DVFs and let $\mathbf{BAM} = \mathrm{B} \cdot \mathbf{FAM}$, then it can be shown that $\mathbf{BQP} \subseteq \mathbf{BAM} \subseteq \mathbf{BUM} \subseteq \mathbf{AWPP}$.

We suspect that all these containments are proper, although we have no evidence as yet to suggest that they are. We also know of no interesting, natural problems in the intermediate classes **BUM** of **BAM** that are not known to be in previously studied subclasses. These are topics for future research.

These results are still in draft form. Technical difficulties with the notation and exposition have delayed submitting this paper to a journal.

Our investigation was also helped by a separate technical improvement in the characterization of **AWPP**. We simplified the definition of **AWPP** using a Gap**P** amplification technique, showing that **AWPP** is a very robust class [Fen03c].

2.2 Noninclusion of NP in BQP

We obtained no noteworthy results related to this question, or the more general question of where **BQP** sits with regard to the polynomial hierarchy. This question is widely acknowledged to be difficult.

2.3 Power of Small-Depth Quantum Circuits

We have a lower bound in this area. We have shown that the quantum fanout operator cannot be computed (even approximately) by sub-logarithmic depth quantum circuits with unbounded fanin AND gates (generalized Toffoli gates) and a sublinear number of ancilla qubits [FFG$^+$06]. The same result holds for the quantum parity operator or any quantum Mod$_k$ operator by results Green et al. [GHMP02].

The *parity operator* on n qubits takes the computational basis state $|x_1, \ldots, x_{n-1}, x_n\rangle$ to $|x_1, \ldots, x_{n-1}, x_1 \oplus \cdots \oplus x_n\rangle$, where x_n is the target and the rest are control qubits. The n-qubit *fan-out operator* takes $|x_1, x_2, \ldots, x_n\rangle$ to $|x_1, x_1 \oplus x_2, \ldots, x_1 \oplus x_n\rangle$, where x_1 is the control and the rest are target qubits. The n-qubit AND gate (generalized Toffoli gate) takes $|x_1, \ldots, x_{n-1}, x_n\rangle$ to $|x_1, \ldots, x_{n-1}, (x_1 \wedge \cdots \wedge x_{n-1}) \oplus x_n\rangle$. Let $\phi = (1+\sqrt{5})/2$ be the golden ratio. In [FFG$^+$06] we prove

Theorem 2.5. *Let C be an n-input quantum circuit of depth d consisting of single-qubit gates and unbounded fan-in quantum AND gates, with a many ancilla qubits.*

- *If C cleanly computes the parity operator, then $d \geq \log_\phi(n/(a+1)) - 1 \doteq 1.44 \log_2(n/(a+1)) - 1$.*
- *If $a = 0$ and C approximates the parity operator to within $1/\sqrt{2}$ in the operator norm, then $d \geq \log_\phi n - 1 \doteq 1.44 \log_2 n - 1$.*

This theorem suggests that the class $\mathbf{QAC}^0$ (the quantum analog of the circuit class $\mathbf{AC}^0$ of constant-depth polynomial-size Boolean circuits with unbounded fan-in AND gates) is properly contained in the class $\mathbf{QAC}^0_{wf} = \mathbf{QACC}^0$ (wf means "with fan-out gates"; $\mathbf{QACC}^0$ is the quantum analog of the circuit class $\mathbf{ACC}^0$ of constant-depth polynomial-size Boolean circuits with unbounded fan-in AND and Mod$_k$ gates). This is certainly the case if the number of ancilla qubits is restricted.

It is straightforward to compute parity in depth $2\log_2 n + 1$ with only controlled NOT gates and no ancilla qubits. We conjecture that this is optimal regardless of how many ancilla qubit are allowed. Thus Theorem 2.5 leaves much room for improvement.

2.4 Simulating Small-Depth Quantum Circuits

We obtained both lower and upper bounds on the difficulty of simulating constant-depth quantum circuits with bounded fan-in gates [FGHZ05]. A family of quantum circuits is in $\mathbf{QNC}^0$ if the circuits in the family have polynomial size and depth $O(1)$, and their gates are drawn from a fixed finite set. This is the analog of families of constant-depth classical Boolean circuits with bounded fan-in gates. Using $\mathbf{QNC}^0$ circuits, we can define language classes such as $\mathbf{NQNC}^0$, the class of languages recognized by $\mathbf{QNC}^0$ circuits where the criterion for acceptance is that the all-zero output state $|00\cdots 0\rangle$ occurs with positive probability. $\mathbf{NQNC}^0$ is the constant-depth analog of the class $\mathbf{NQP}$ defined in [ADH97], which is equal to the counting class $\mathbf{C}_{\neq}\mathbf{P}$ [FGHP99, YY99]. In [FGHZ05] we improved on a construction of Terhal & DiVincenzo [TD04] to show

Theorem 2.6. $\mathbf{NQNC}^0 = \mathbf{NQP} = \mathbf{C}_{\neq}\mathbf{P}$.

Thus deciding zero versus nonzero output probabilities for a given state is just as hard for constant-depth quantum circuits as it is for arbitrary quantum circuits, and the latter task is known to be hard for the polynomial hierarchy (see [FGHP99]). This is true even for circuits of depth just three (which is optimal [TD04]).

In the other direction, we also showed that acceptance probabilities for $\mathbf{QNC}^0$ circuits can be computed *approximately* in (classical) polynomial time [FGHZ05]. This implies that certain bounded-error language classes defined from $\mathbf{QNC}^0$ circuits are contained in $\mathbf{P}$. For $0 < \epsilon \le \delta \le 1$, we define $\mathbf{BQNC}^0_{\epsilon,\delta}$ to be the class of languages recognized by polynomial-time uniform families of constant-depth, polynomial-size quantum circuits with acceptance probability either $< \epsilon$ (for rejection) or $\ge \delta$ (for acceptance). The values ϵ and δ may be functions of the circuit. (The *acceptance probability* of a circuit is the probability of observing the output qubits to be all zero.) In [FGHZ05] we show that

Theorem 2.7. *If* $1 - \epsilon \ge 4^d(1 - \delta)$ *where* d *is the circuit depth, then* $\mathbf{BQNC}^0 \subseteq \mathbf{P}$.

This upper-bound result can stand improvement in two ways: (i) decreasing the gap between $1 - \epsilon$ and $1 - \delta$ to a factor significantly less than 4^d, and (ii) loosening the definition of $\mathbf{QNC}^0$ by allowing nontrivial classical postprocessing before deciding acceptance.

2.5 New Quantum Primitives

In two separate papers we considered spin-exchange interactions between n spin-1/2 particles, where the pairwise couplings are all equal. In the first paper [Fen03b], we considered the Hamiltonian $H_z = J_z^2$, where J_z is the operator giving the total spin in the z-direction. In the second paper [FZ04], we considered the more isotropic Heisenberg interaction, with a parameterized Hamiltonian of

$$H_{\alpha,\beta} = -J^2 + \alpha J_z + \beta J_z^2,$$

where α and β are any real constants with $\beta \ne 1$, and $J^2 = J_x^2 + J_y^2 + J_z^2$ is the squared magnitude of the total spin. This investigation was prompted by questions posed by Chuang [Chu03, Chu04].

In each of these papers, we showed that, for any $n > 0$, the spin-exchange interaction can be used to exactly implement an n-qubit parity gate, which is equivalent in constant depth to an n-qubit fanout gate. In the earlier paper, each qubit is a single spin-1/2 particle, with no encoding needed. In the later paper, we need to encode each qubit into a pair of spin-1/2 particles.

We generalized our basic results by showing that any Hamiltonian (acting on suitably encoded logical qubits), whose eigenvalues depend quadratically on the Hamming weight of the logical qubit values, can be used to implement generalized Mod_q gates for any $q \ge 2$.

The circuit for parity from the second paper is shown in Figure 1. Here, the gate E, depicted in Figure 2, encodes a qubit into a pair of particles, sending $|0\rangle$ to $|00\rangle$ and sending $|1\rangle$ to the singlet state $(|10\rangle - |01\rangle)/\sqrt{2}$. Since $E = E^\dagger$, it is also used for decoding at the end. The gate H is the one-qubit Hadamard operator. The U operator represents the Heisenberg interaction being turned on for a period of time $t = \pi/(2|\beta - 1|)$; that is,

$$U = e^{-itH_{\alpha,\beta}}.$$

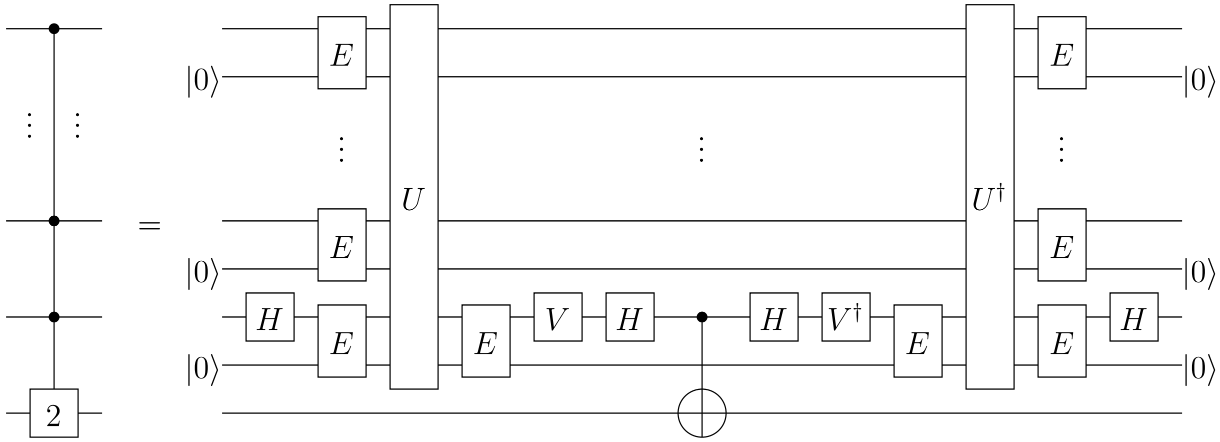

Figure 1: Circuit to implement parity with Heisenberg interactions.

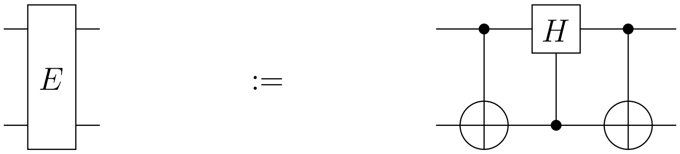

Figure 2: A two-qubit encoder.

Finally, V is a conditional phase shift gate:

$$V = \begin{bmatrix} 1 & 0 \\ 0 & e^{-is\pi(2r+\gamma-1)/2} \end{bmatrix},$$

where r is the number of control qubits of the parity gate on the left-hand side of Figure 1, $\gamma = (\alpha - 1)/(\beta - 1)$, and $s = 1$ if $\beta > 1$ and $s = -1$ otherwise. More details are in [FZ04].

One hopes that parity and fan-out operators (which are surprisingly powerful for constant-depth quantum computation [HŠ03]) can be implemented on a modest scale using this interaction. Ion traps may allow for this, in that certain processes may be able to communicate spin couplings evenly across the particles.

The circuit of Figure 1 seems to be inherently fault-intolerant, which presents an obstacle for larger-scale implementations. Also, we have assumed throughout that the coupling coefficients are all equal. Whether this assumption is realistic remains to be seen. It is certainly more likely in the short run that in feasible laboratory setups, the coefficients will not be equal, but can still satisfy certain symmetries.

2.6 New Quantum Algorithms

We have shown that there are efficient quantum algorithms for certain problems on groups, namely, Group Intersection and Double Coset Membership (defined below), by reducing them to previously studied problems for which efficient quantum algorithms are known [FZ05].

Our work applies to the black-box group model of Babai & Szemerédi [BS84]. In this model, a family of groups $B_1, B_2, B_3, \ldots$ is assumed, where the elements of each B_n are represented by strings of length polynomial in n, and where the group operation and inverse map on B_n is given by an oracle. The B_n are sometimes called "ambient groups." Group-theoretic algorithms in this model may take as inputs elements and subgroups of B_n and use the oracle to compute products and inverses. A subgroup $H \leq B_n$ is always represented for computational purposes by a list of generators for H of length $O(\log n)$. Black-box group algorithms are general in the sense that any concrete implementation of the group oracle (e.g., matrix groups or permutation groups) immediately yields concrete implementations of the algorithms.

The model may or may not assume that group elements are encoded by unique strings. If not, then an equality-testing oracle is also assumed (testing whether two strings represent the same group element). Our work relates to the unique encoding model, although we need results from the non-unique model in order to handle factor groups.

The following definitions of some group theoretic decision problems are adapted from Arvind & Vinodchandran [AV97].

Definition 2.8 ([AV97]). *Let $\mathcal{B} = \{B_n\}_{n\geq 1}$ be a group family. Let e denote the identity element of each B_n. Below, g and h denote elements, and S_1 and S_2 subgroups, of B_n.*

$$\begin{aligned}
\textsc{Group Intersection} &:= \{(0^n, S_1, S_2) \mid S_1 \cap S_2 = \{e\}\}, \\
\textsc{Multiple Group Intersection} &:= \{(0^n, S_1, \ldots, S_k) \mid S_1 \cap \ldots \cap S_k = \{e\}\}, \\
\textsc{Group Membership} &:= \{(0^n, S_1, g) \mid g \in S_1\}, \\
\textsc{Group Factorization} &:= \{(0^n, S_1, S_2, g) \mid g \in S_1 S_2\}, \\
\textsc{Coset Intersection} &:= \{(0^n, S_1, S_2, g) \mid S_1 g \cap S_2 \neq \emptyset\}, \\
\textsc{Double Coset Membership} &:= \{(0^n, S_1, S_2, g, h) \mid g \in S_1 h S_2\}.
\end{aligned}$$

We also studied restrictions of some of these problems, such as Solvable Group Intersection, where the input subgroups are assumed to be solvable.

Figure 3 depicts some efficient quantum reducibility relationships among these and other group-theoretic problems such as Orbit Coset and Orbit Superposition defined by Friedl et al. [FIM+03]. In that paper, a quantum algorithm for Orbit Coset was decribed that runs in polynomial time for *smoothly solvable groups*, i.e., families of input groups that are solvable with abelian decomposition series of length $O(1)$ such that each factor group is the direct product of a group with exponent $O(1)$ and a group of size $(\log n)^{O(1)}$, where n is the index parameterizing the ambient group.

Our reductions immediately imply efficient quantum algorithms for Solvable Group Intersection if one of the underlying solvable groups has a smoothly solvable commutator subgroup, and for Double Coset Membership if one of the underlying solvable groups is smoothly solvable [FZ05]. Our work also introduces new decision versions of some search problems, namely Stabilizer$_D$ and Orbit Coset$_D$, to help with the reducibilities. For

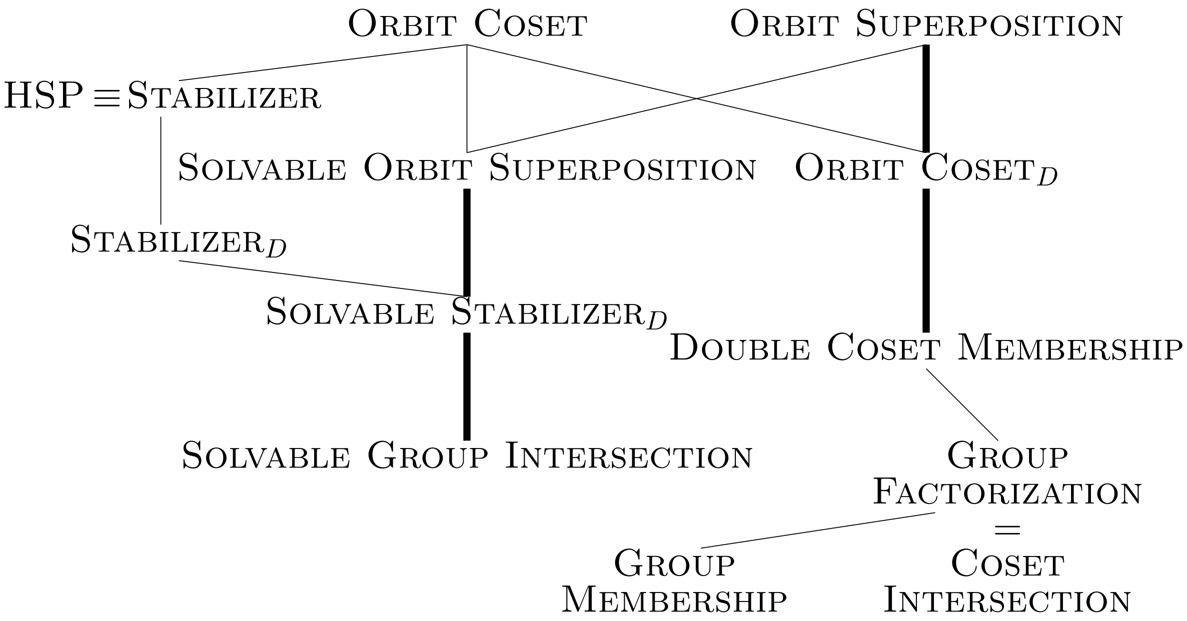

Figure 3: Quantum reducibility relationships between various group-theoretic problems. Thick lines indicate nontrivial reductions we found in [FZ05]

example, whereas Stabilizer asks for (generators of) the stabilizer of a point with respect to a group action, Stabilizer$_D$ merely asks whether or not the stabilizer is trivial. It is an interesting question to ask if these decision problems are strictly easier than their search versions. This is an area of continued investigation.

We have also shown that Group Intersection and Double Coset Membership have statistical zero-knowledge proofs [FZ05].

2.7 New Quantum Communication Protocols

We have investigated some problems in quantum communication, but currently have nothing significant to report.

2.8 Quantum Random Walks

Although we did not propose work on this problem, we have a modest result in the area of quantum random walks [FZ03]. We improve the analysis of an exponential lower bound on the best expected time of a classical algorithm solving a random walk problem for which a polynomial-time quantum algorithm has been found by Childs et al. [CCD$^+$03].

References

[ADH97] L. M. Adleman, J. DeMarrais, and M.-D. A. Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997.

[AKN98] D. Aharonov, A. Yu. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings of the 30th ACM Symposium on the Theory of Computing*, pages 20–30, 1998, quant-ph/9806029.

[AV97] V. Arvind and N. V. Vinodchandran. Solvable black-box group problems are low for PP. *Theoretical Computer Science*, 180:17–45, 1997.

[BS84] L. Babai and E. Szemerédi. On the complexity of matrix group problems I. In *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science*, pages 229–240, 1984.

[CCD$^+$03] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman. Exponential algorithmic speedup by a quantum walk. In *Proceedings of the 35th ACM Symposium on the Theory of Computing*. ACM, 2003, quant-ph/0209131.

[Chu03] I. L. Chuang, 2003. Private communication.

[Chu04] I. L. Chuang, 2004. Private communication.

[Fen03a] S. A. Fenner. Distribution-valued functions and quantum computation. Preliminary draft, 2003.

[Fen03b] S. A. Fenner. Implementing the fanout gate by a Hamiltonian, 2003, quant-ph/0309163. Manuscript.

[Fen03c] S. A. Fenner. PP-lowness and a simple definition of AWPP. *Theory of Computing Systems*, 36:199–212, 2003. Also available as ECCC Report TR02-036.

[FFG$^+$06] M. Fang, S. Fenner, F. Green, S. Homer, and Y. Zhang. Quantum lower bounds for fanout. *Quantum Information and Computation*, 6:46–57, 2006, quant-ph/0312208.

[FFK94] S. Fenner, L. Fortnow, and S. Kurtz. Gap-definable counting classes. *Journal of Computer and System Sciences*, 48(1):116–148, 1994.

[FFKL03] S. Fenner, L. Fortnow, S. Kurtz, and L. Li. An oracle builder's toolkit. *Information and Computation*, 182:95–136, 2003.

[FGHP99] S. Fenner, F. Green, S. Homer, and R. Pruim. Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy. *Proceedings of the Royal Society London A*, 455:3953–3966, 1999, quant-ph/9812056.

[FGHZ05] S. Fenner, F. Green, S. Homer, and Y. Zhang. Bounds on the power of constant-depth quantum circuits. In *Proceedings of the 15th International Symposium on Fundamentals of Computation Theory*, volume 3623 of *Lecture Notes in Computer Science*, pages 44–55. Springer-Verlag, 2005, quant-ph/0312209.

[FIM$^+$03] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen. Hidden Translation and Orbit Coset in quantum computing. In *Proceedings of the 35th ACM Symposium on the Theory of Computing*, pages 1–9, 2003, quant-ph/0211091.

[FR99] L. Fortnow and J. Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999, cs.CC/9811023.

[FZ03] S. Fenner and Y. Zhang. A note on the classical lower bound for a quantum walk algorithm. Manuscript, 2003, quant-ph/0312230.

[FZ04] S. Fenner and Y. Zhang. Implementing fanout, parity, and mod gates via spin exchange interactions, 2004, quant-ph/0407125. Manuscript.

[FZ05] S. Fenner and Y. Zhang. Quantum algorithms for a set of group theoretic problems. In *Proceedings of the 9th IC-EATCS Italian Conference on Theoretical Computer Science*, volume 3701 of *Lecture Notes in Computer Science*, pages 215–227. Springer-Verlag, 2005, quant-ph/0408150.

[GHMP02] F. Green, S. Homer, C. Moore, and C. Pollett. Counting, fanout and the complexity of quantum ACC. *Quantum Information and Computation*, 2:35–65, 2002, quant-ph/0106017.

[HŠ03] P. Høyer and R. Špalek. Quantum circuits with unbounded fan-out. In *Proceedings of the 20th Symposium on Theoretical Aspects of Computer Science*, volume 2607 of *Lecture Notes in Computer Science*, pages 234–246. Springer-Verlag, 2003.

[Li93] L. Li. On the counting functions. Technical Report TR-93-12, The University of Chicago, 1993. PhD thesis, available at http://www.cs.uchicago.edu/research/publications/techreports/TR-93-12.

[Pap94] C. H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[TD04] B. M. Terhal and D. P. DiVincenzo. Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games. *Quantum Information and Computation*, 4(2):134–145, 2004.

[YY99] T. Yamakami and A. C.-C. Yao. $\mathrm{NQP}_{\mathbf{C}} = \text{co-}\mathrm{C}_{=}\mathrm{P}$. *Information Processing Letters*, 71(2):63–69, 1999, quant-ph/9812032.